SECRET

CMC-5

DIRECTOR OF CENTRAL INTELLIGENCE

Security Committee

SECOM-A-260

20 December 1983

AGENDA
Two Hundred and Sixty-ninth Meeting
Wednesday, 11 January 1983, 10:00 a.m.
Room 2E465 Pentagon

(Please see attached fact sheet and map for directions)

Special Briefing

Computer Security Briefing by Dr. Ruth Davis (members are encouraged to determine beforehand the positions on computer security of their departments and agencies so they will be fully prepared for this presentation)

Preliminary Comments

ITEM 1 Approval of Minutes of 16 November 1983 Meeting

ITEM 2 Subcommittee Reports

Personnel Security
Unauthorized Disclosures Investigations

ITEM 3 Proposed charter for the Unauthorized Disclosures Investigations Subcommittee (member decision on the attached draft)

ITEM 4 SECOM Goals and Objectives for 1984 (see attached copy of memorandum sent to Director, Intelligence Community Staff)

ITEM 5 New Business

ITEM 6 Next Meeting

Attachments

OFFICIAL USE ONLY When
Classified Attachment Removed

FACT SHEET FOR THE 11 JANUARY 1984 SECOM MEETING

1. PARKING: For your own convenience you are encouraged to take public transportation. You may have a difficult time finding parking that is close to the building. There are two areas where you may park:

a. The E-1 Parking Lot for visitors, beginning 1 January 84, will be open at 0900 hours daily and will charge .25¢ per hour. This lot will fill up quickly. To find this Lot follow the signs for "Visitor Parking".

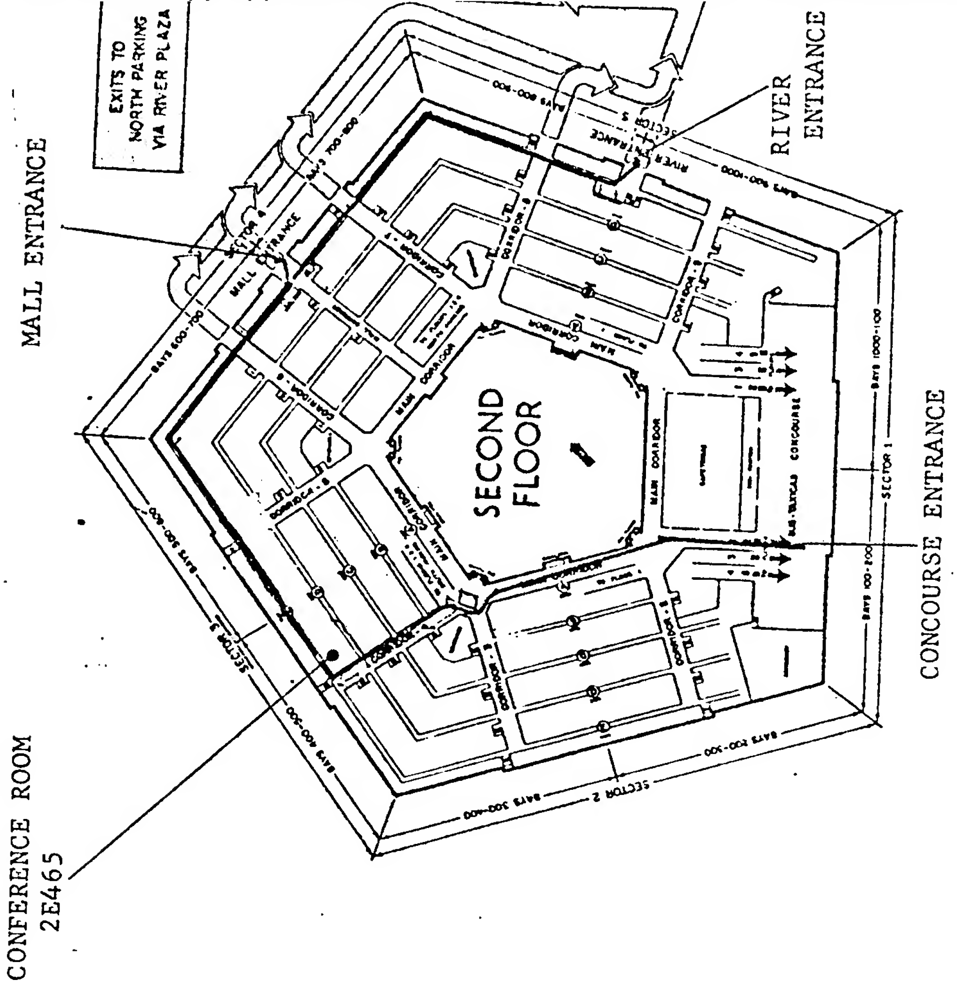
b. Mid-Town Parking is at the far end of Pentagon North Parking and is a commercial enterprise. The cost is $1.50 per day or any portion of the day. Parking is normally available. To find this Lot follow the signs to "North Parking".

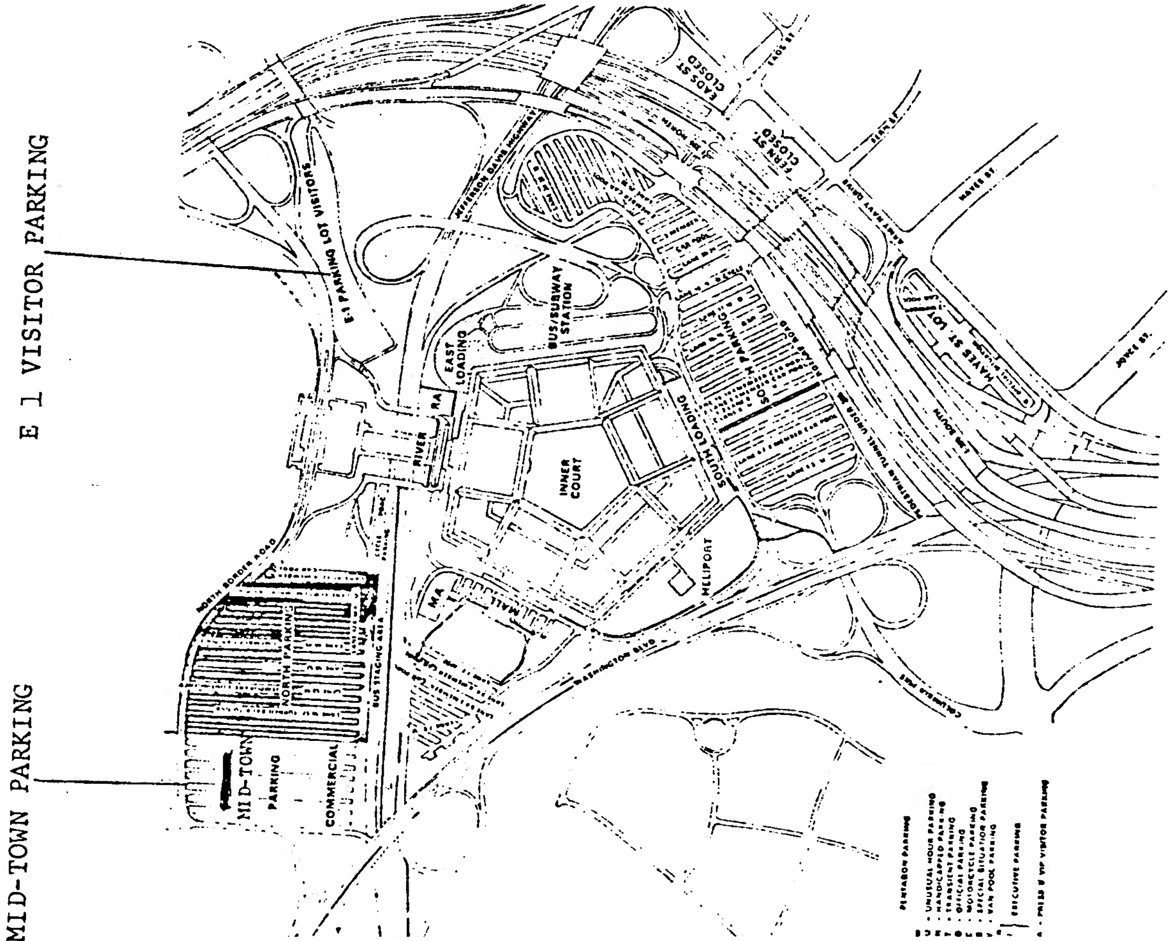
2. DIRECTIONS: The meeting will be held in the OACSI Conference Room; Rm # 2E465, Telephone 695-6588. 2E465 is on the second floor, E ring, between Corridors four and five.

a. If you take public transportation you will enter through the Concourse. Go to the left side of the Concourse (your left as you face the entrances) and enter thru "Ramps to Floors 1 & 2". Proceed straight ahead thru the "Anzus" and "Faces of War" Corridors and around a large pillar to Corridor 4. Follow Corridor 4 to the end (this is E Ring) and take a right. 2E465 will be one door up on your right. See Map.

b. If entering from the River or Mall entrances take an immediate right (this is E Ring) and proceed around the Ring until you reach 2E465 on your left. See Map.

3. You should be able to enter the Pentagon with any Government agency ID card. If there are any problems gaining access or if you have any questions please contact Major Charles D. Lurey or Mrs Clarice Vincent at 697-3934/Autovon 227-3934.


EXITS TO NORTH PARKING VIA RIVER PLAZA
MALL ENTRANCE
RIVER ENTRANCE
SECOND FLOOR
CONCOURSE ENTRANCE
CONFERENCE ROOM 2E465
SECTOR 1
SECTOR 2
SECTOR 3
SECTOR 4
SECTOR 5
MALL ENTRANCE
RIVER ENTRANCE
MAIN CORRIDOR
CONCOURSE
BAYS 100-200
BAYS 200-300
BAYS 300-400
BAYS 400-500
BAYS 500-600
BAYS 600-700
BAYS 700-800
BAYS 800-900
BAYS 900-1000
BAYS 1000-100


E 1 VISITOR PARKING
MID-TOWN PARKING
E-1 PARKING LOT VISITORS
JEFFERSON DAVIS HIGHWAY
EADS ST CLOSED
FERN ST CLOSED
HAYES ST.
HAYES ST LOT
BUS/SUBWAY STATION
EAST LOADING
RIVER
INNER COURT
SOUTH LOADING
SOUTH PARKING
HELIPORT
MALL
WASHINGTON BLVD
NORTH BORDER ROAD
NORTH PARKING
BUS STAGING AREA
MID-TOWN PARKING
COMMERCIAL
PENTAGON PARKING
UNUSUAL HOUR PARKING
HANDICAPPED PARKING
TRANSIENT PARKING
OFFICIAL PARKING
MOTORCYCLE PARKING
SPECIAL SITUATION PARKING
VAN POOL PARKING
EXECUTIVE PARKING

UNAUTHORIZED DISCLOSURE INVESTIGATIONS SUBCOMMITTEE CHARTER

The Unauthorized Disclosure Investigations Subcommittee operates under the authority of section 2.c and 4 of the Director of Central Intelligence Directive: Security Committee, effective 15 July 1982. In order to better delineate the missions, functions, responsibilities, and organization of the Subcommittee, the following provisions are established.

1. Mission: The Unauthorized Disclosure Investigations Subcommittee will advise and assist the Security Committee in discharging its responsibilities to ensure that programs are developed which protect intelligence sources and methods, and classified intelligence from unauthorized disclosure. The major focus of attention is on analysing and preventing such disclosures.

2. Functions: Under the general guidance of the Security Committee, the Subcommittee will perform the following functions:

a. Advise the Security Committee on security policies and procedures to ensure the implementation of the policies of the Director of Central Intelligence regarding the prevention of unauthorized disclosures of classified intelligence and intelligence sources and methods.

b. Recommend to the Security Committee policies for the conduct by intelligence community components of security investigations of unauthorized disclosures of classified intelligence and intelligence sources and methods.

c. Recommend to the Security Committee policies, procedures, and standards regarding those cases of unauthorized disclosures of classified intelligence or intelligence sources and methods which may appropriately be referred by Federal agencies to the Attorney General for FBI investigation.

d. Recommend to the Security Committee policies, procedures, and standards regarding the application of appropriate sanctions in cases where investigation clearly identifies an employee, contractor or other Federal official who was responsible for an unauthorized disclosure of classified intelligence or intelligence sources and methods.

e. Determine and recommend to the Security Committee corrective security measures to preclude the recurrence of disclosure or compromise of classified intelligence and intelligence sources and methods.

f. Determine and recommend to the Security Committee methods to increase security education and awareness regarding unauthorized disclosures of classified intelligence and intelligence sources and methods.

g. Determine and recommend to the Security Committee improved methods for analyzing unauthorized disclosures of classified intelligence and intelligence sources and methods.

h. Determine and recommend to the Security Committee policies and procedures for coordinating investigative efforts on unauthorized disclosures involving more than one department or agency.

i. Undertake those additional functions concerning the unauthorized disclosures of classified intelligence and intelligence sources and methods as the Security Committee may from time to time direct.

3. Intelligence Community Responsibilities. Members agencies are responsible for providing to the Subcommittee Chairperson information relevant to the Subcommittee's function.

4. Composition and Organization.

a. The Subcommittee Chairperson will be appointed by the Chairman of the Security Committee.

b. The membership of the Subcommittee will be composed of representatives of those government entities represented on the Security Committee.

c. With the consent of affected members, the Subcommittee Chairperson may appoint persons with special skills to provide support to the Subcommittee.

d. There shall be a representative from the Security Committee staff assigned to provide support to the Subcommittee as appropriate. The Subcommittee Chairperson together with the representative from the Security Committee shall coordinate all matters between the Subcommittee and the Security Committee.

e. With the approval of the Security Committee Chairman, the Subcommittee Chairperson may invite representatives of relevant United States Government entities to participate from time to time as appropriate.

SECRET

DIRECTOR OF CENTRAL INTELLIGENCE
Security Committee

SECOM-D-249

14 December 1983

MEMORANDUM FOR: Director, Intelligence Community Staff

FROM: [redacted] 25X1
Chairman

SUBJECT: SECOM Goals & Objectives for 1984 (U)

REFERENCE: D/ICS Memo dated 5 December

In response to the reference, Security Committee's goals and objectives for 1984 are attached.

[redacted] 25X1

Attachment

DCI Security Committee Goals and Objectives for 1984

a. Develop for Community agreement a long range plan to synchronize DCI security policies and procedures for the protection of intelligence sources, methods and information based on current assessment of threats, vulnerabilities and environments.

b. Continue efforts to enhance common Community understanding of effective security requirements and common application of DCI security policies and procedures. In support of this, seek to upgrade Community personnel clearance practices for access to non-SCI intelligence information, while ensuring that the highest standards are maintained for SCI access.

c. Thoroughly review collection requirements on subjects of vital interest to SECOM and its subcommittees; ensure that new or revised tasking is formulated as needed. Encourage the Community to establish analysis centers to evaluate security-related data.

d. Develop a seminar for SECOM members on personnel security studies and research; psychological profiles of spies, defectors and leakers; and innovative approaches to determining personnel reliability. Consider SECOM sponsorship of an effort to develop data on common personality traits of U.S. citizens who commit espionage.

e. Gather anecdotal data on the value of the polygraph in personnel security screening; make sanitized material on actual cases available to those responsible for decisions on continued or expanded use of the polygraph; encourage studies of possible measures to defeat the polygraph.

f. Develop a standard procedure for Community agencies to use in reporting to the Information Security Oversight Office on unauthorized disclosures of classified intelligence.

g. Develop Community standards to identify and record common data on unauthorized disclosures of intelligence, seek Community agreement for a SECOM-sponsored common data base, and develop a mechanism to conduct ongoing analysis of leaks.

h. Conduct four Community seminars each for SCI personnel security adjudicators and for physical security officers, updating both series to keep abreast of Community needs and to enhance common application of DCI security standards.

i. Encourage more and better use of existing security education material, such as the DCI videotape on leaks, the SECOM-developed Security Orientation for Senior Officials, and DIA videotapes on leaks and hostile espionage. Develop and produce at least one new videotape on a security education theme.

j. Through the SECOM Physical Security Working Group (PSWG), arrange to evaluate new physical security equipment, using the resources of the General Services Administration's Interagency Advisory Committee on Protective Equipment or the capabilities of the PSWG members, as appropriate. Establish a mechanism to approve or endorse new physical security equipment for use in protecting compartmented or classified intelligence.

k. Encourage the Community to commit more effort and resources to R&D on techniques and equipment to identify and counter hostile technical attacks. Continue to seek "seed money" for use in initiating or sustaining security R&D.

l. Complete the revision of the DCI regulation on "Security of Foreign Intelligence Information in Automated Systems and Networks" taking full account of the results of Dr. Ruth Davis's study.

m. Continue to coordinate Community support to the FBI's efforts to assist in enhancing technical security on Capitol Hill.